Shibboleth based Authentication, Authorization, Accounting and Auditing in Wireless Mesh Networks

Schiller, Eryk ; Monakhov, Alexey ; Kropf, Peter

Abstract: We present the basic architectural elements of the Captive Portal integrating Shibboleth based Authentication, Authorization, Accounting and Auditing into Wireless Mesh Networks. The Captive Portal is built upon the SWITCHaai/Shibboleth architecture especially designed to protect web based services. The architecture is secure, eavesdropping protected and does not require any specialized software installation on the client side.

DOI: https://doi.org/10.1109/LCN.2011.6115572

Shibboleth based Authentication, Authorization, Accounting and Auditing in Wireless Mesh Networks

Eryk Schiller, Alexey Monakhov and Peter Kropf
University of Neuchatel
Switzerland
Email: {eryk.schiller, alexey.monakhov, peter.kropf}@unine.ch

***Abstract*—We present the basic architectural elements of the Captive Portal integrating Shibboleth based Authentication, Authorization, Accounting and Auditing into Wireless Mesh Networks. The Captive Portal is built upon the SWITCHaai/Shibboleth architecture especially designed to protect web based services. The architecture is secure, eavesdropping protected and does not require any specialized software installation on the client side.**

I. Introduction

In this paper, we present an architecture of the Authentication, Authorization, Accounting and Auditing capable Wireless Mesh Network built out of wireless Local Area Networks (LANs).

A. Requirements

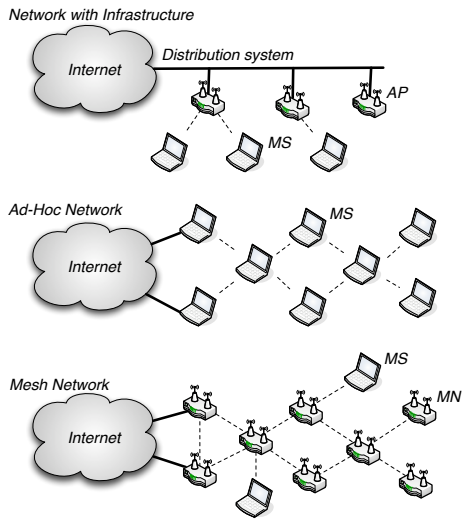

Figure 1. Wireless Networks

We start by describing the context of this work: Wireless Mesh Networks (WMNs), a current state of Authentication, Authorization and Accounting (AAA) and our main goal: an integration of AAA into WMNs.

1) Wireless Networks: In Figure 1, we present the most prominent examples of wireless networks: infrastructure networks, ad-hoc networks and finally WMNs.

In infrastructure networks, we distinguish Mobile Stations (MSs), Access Points (APs) and a wired Distribution System (DS). MSs equipped with wireless interfaces connect to APs having both wireless and wired interfaces. Every AP connected to a wired DS provides access to the Internet. Each AP forwards traffic between a MS and the DS. Consequently, the MS benefits from single hop wireless connectivity obtaining the access to the Internet.

In ad-hoc networks, there is no distinction between a MS and an AP and the DS does not exist. MSs communicate with each other by using their wireless interfaces. To provide multi-hop communication, a network runs a routing protocol. MSs can communicate even if they are not directly connected, because intermediate nodes on the path between communicating MSs forward information. Some of the MSs may provide access to the Internet sharing their Internet connection with other MSs in the ad-hoc network.

A WMN can be considered as a wireless network lying in between infrastructure networks and ad-hoc networks [1]. A WMN distinguishes Mesh Nodes (MNs) and MSs, but the wired DS does not exist. The information is propagated by using the wireless interfaces in a multi-hop manner. MNs are more stable than MSs meaning they do not move frequently and have longer up-times. MNs form a wireless backhaul and they exchange information by using wireless interfaces. To implement a multi-hop propagation of information, a wireless backhaul runs a routing protocol. MSs get connectivity to the network by using their wireless interfaces, associating themselves with MNs. Normally, MSs are not involved in the routing operation, they are client terminals of a WMN. A wireless backhaul connected to the Internet may offer an Internet connection to MSs.

A WMN is a low cost complement or an extension to the wired Internet [2], because it does not require establishing a wired infrastructure. The WMN providing a signal should have similar characteristics to wired networking in terms of accessibility, reliability, robustness and performance.

A wired network is highly reliable and built out of expensive, robust, reliable, high performance routers especially

designed for packet forwarding. Accessibility of these systems often exceeds 99%. Wired network adapters are very reliable so that packets are almost not affected by losses due to signal propagation. They operate with fixed link capacities delivering a signal on large distances with high data rates. If a link fulfills the technical requirements of the device, it is able to achieve a desired throughput. High performance routing protocols deal with route failures and automatically redirect traffic to backup routes in case of link problems.

Wireless Networks are different. A WMN is a perfect solution for last mile connectivity because of its low cost and ease of use, however, a single hop, long range operation is difficult to manage due to signal propagation conditions, attenuation and timescales introduced by MAC layers. Because of all these problems, we are enforced to send data in a multi-hop manner in which MNs push packets closer their destinations. Wireless links are lossy and highly affected by the signal propagation conditions and MAC interactions. The link capacity is not well defined. It depends on the link length, signal strength, noise level, interferences, changing weather conditions (e.g., precipitation, humidity, fog, pollution), collisions, topological problems (e.g., hidden, exposed node problems), etc. As a consequence, routing protocols must deal with many factors that do not exist in wired networks, so the path selection process is very complex and yet not well understood. Wireless mesh nodes are often not so powerful and reliable as high performance wired routers. Because of all above situations, building a high performance WMN is a challenge. Wireless Mesh Networking should be able to provide the same services as wired networking meaning data, voice and video transmissions with similar quality of service.

2) AAA in wireless networks: There exist many wireless infrastructure networks giving access to the Internet (cf., Figure 2). The most important disadvantage of an infrastructure network is that each AP requires a wired connection that limits the network range to areas in which the infrastructure already exists and increases operational costs, because a cabled infrastructure is expensive. To protect the Internet connection against unauthorized users, only a limited number of services is available immediately after a MS associates itself with an AP. Normally, a MS can only communicate with Virtual Private Network (VPN) servers, Wi-Fi Protected Access II (WPA2) [3] running APs and Captive Portals. The VPN mode of operation is out of scope of this paper. We only focus on WPA2 APs and Captive Portals based on the The Internet Engineering Task Force (IETF) Network Access Server (NAS) model described in [4], [5]. Based on the IETF NAS model, each service providing access to the Internet deals with the following functionalities:

- "Authentication refers to the confirmation that a user who is requesting services is a valid user of the network services requested. Authentication is accomplished via the presentation of an identity and credentials. Examples of types of credentials are passwords.
- Authorization refers to the granting of specific types of service (including no service) to users, based on their authentication, what services they are requesting, and the current system state.
- Accounting refers to the tracking of the consumption of NAS resources by users. This information may be used for management, planning, billing, or other purposes.
- Auditing refers to the tracking of activity by users. As opposed to accounting, where the purpose is to track consumption of resources, the purpose of auditing is to determine the nature of a user's network activity. Examples of auditing information include the identity of the user, the nature of the services used, what hosts were accessed when, what protocols were used, etc."

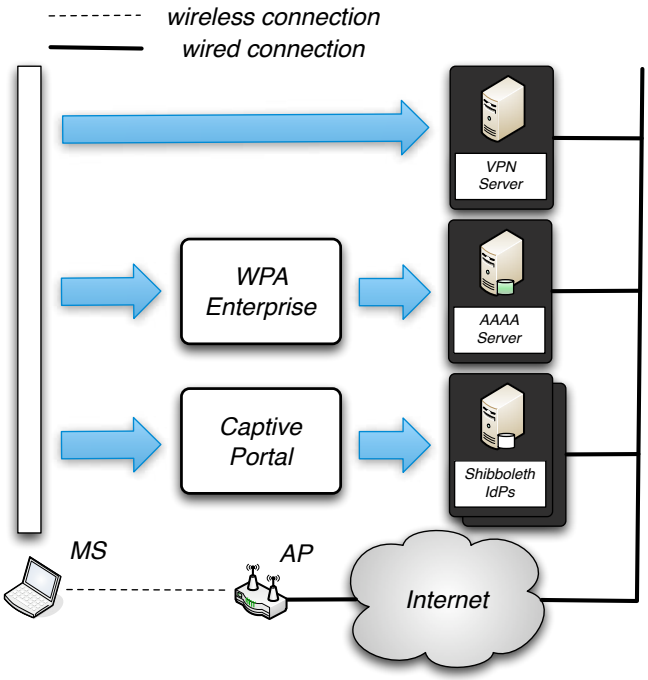

Figure 2. Current state of AAA oriented networking

For the rest of this paper, we use the definitions of Authentication, Authorization, Accounting and Auditing described above. The well known network architecture based on, e.g., WPA2/Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS) [6], [7] and a Remote Authentication Dial-In User Service (RADIUS) [8] server (cf., Figure 3) supports Authentication, Authorization, Accounting and Auditing (AAAA). We will briefly describe the network operation. In the first step, a MS authenticates the RADIUS server by using a digital certificate. This operation protects the MS against communication with a malicious server. When the server is trusted, a secured tunnel between the MS and the RADIUS server is established. The tunnel is secured by means of strong public/private key cryptography and allows the MS to send its credentials in a secure manner. The RADIUS server issues a Master Key (MK) when MS is successfully authenticated and authorized. A copy of the key goes to the MS. The MS and the RADIUS server derive a Primary Master Key (PMK) by

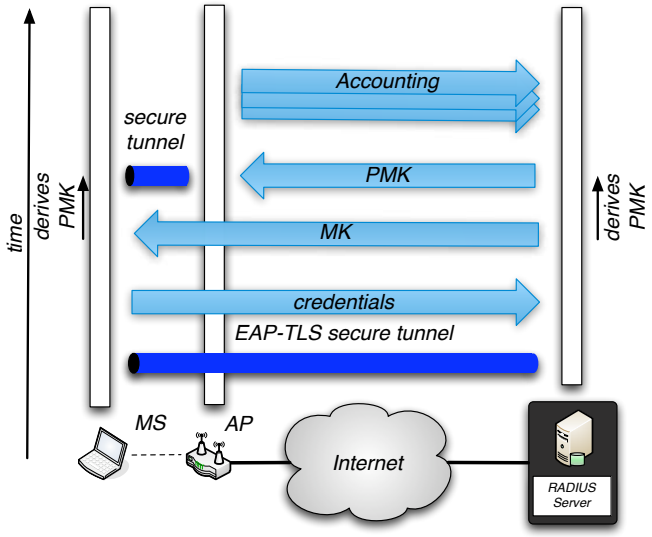

Figure 3. WPA2/EAP-TLS with RADIUS

using the MK and a hashing function. The RADIUS server sends the PMK to the AP. In this phase the AP and the MS both have a copy of the PMK being a symmetric master key for future secure communication. Once, a secure tunnel between the AP and the MS is established, the MS can use the Internet connection. The AP assumes that the data exchanged by the MS-AP tunnel belongs to the legitimate MS (because only the MS and the AP know the PMK). Consequently, the AP can gather statistics on the MS-AP tunnel activity, e.g., sent and received traffic, etc. and then issues accounting messages to the RADIUS server [9]. Accounting information serves for future auditing and billing.

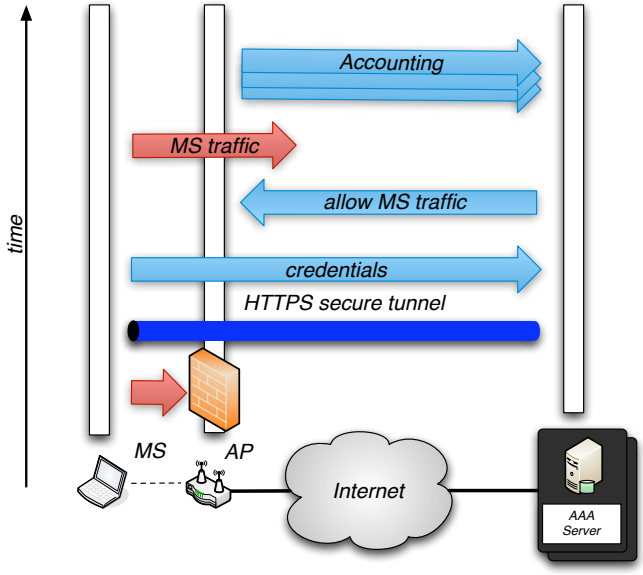

Figure 4. Captive Portal

The Captive Portal is another possible solution. We use it, because it is simple and does not require any additional protocols like EAP, etc. A MS does not need to provide any sophisticated software to join the network. An architecture of the Captive Portal is built upon the NAS AAA paradigm (cf., Figure 4). At the beginning of operation a MS associates with an AP. The MS gets the network address, but its traffic is blocked at the AP by some sort of a firewall. Each time the MS issues a Hypertext Transfer Protocol (HTTP) request, it is redirected to an AAA server in order to establish secure connection. Once a secure Hypertext Transfer Protocol Secure (HTTPS) tunnel is established, the MS is requested to authenticate itself by presenting credentials. If the AAA server successfully authenticates and authorizes the MS to use network resources, the server requests the AP to reconfigure its firewall and allow MS' traffic. The traffic is recognized by the MS' network and link layer addresses. Starting from this point, the MS has full access to the Internet. The AP can bookkeep traffic originated at or destined to the MS and issues the accounting messages to the AAA server.

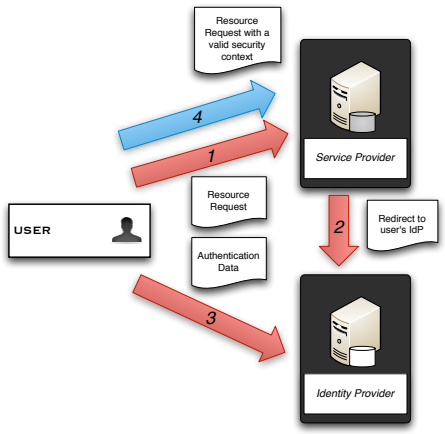

Figure 5. Shibboleth architecture

Because each Captive Portal is a service with a web-based interface, one can replace an AAA server with the SWITCHaai architecture [10], [11] especially designed to protect web services. The disadvantage of this solution is that, at the moment, SWITCHaai does not natively support accounting [1]. The big advantage is that the architecture is simple and fits well the Captive Portal paradigm.

We describe the architecture of SWITCHaai/Shibboleth being one of the most prominent Authentication Authorization Infrastructure (AAI) mechanisms for educational institutions. The current Shibboleth AAI architecture consists of the following interconnected entities: "User", "Service Provider" and "Identity Provider".

A user is a human being operating a computing device (e.g., a personal computer or a laptop) interconnected by a network with other entities. A Service Provider manages protected

[1]The implementation of the accounting functions is under development and expected to become operational soon.

resources (e.g., an online library secured against unauthorized users) and decides whether a user is authorized to access a resource or not. Decisions are based on assertions being delivered by Identity Providers (IdPs). The role of an IdP is to deliver a security context to the Service Provider (SP). The security context depends on credentials presented by a user to the IdP.

We illustrate the authentication and authorization process in Figure 5. A user asks a SP for a particular resource. When the SP does not have a valid security context, the user is redirected to its home organization IdP to authenticate itself against an IdP. The IdP creates a security context at the SP and redirects the user once again to the SP. As the security context exists at the SP, the SP may authorize a user to access the resource. This method has many advantages, e.g., the user authenticates itself against his own IdP, so the important data is not shared with third parties. SPs only get the parameters needed for a user authorization process and they do not see the sensitive credentials.

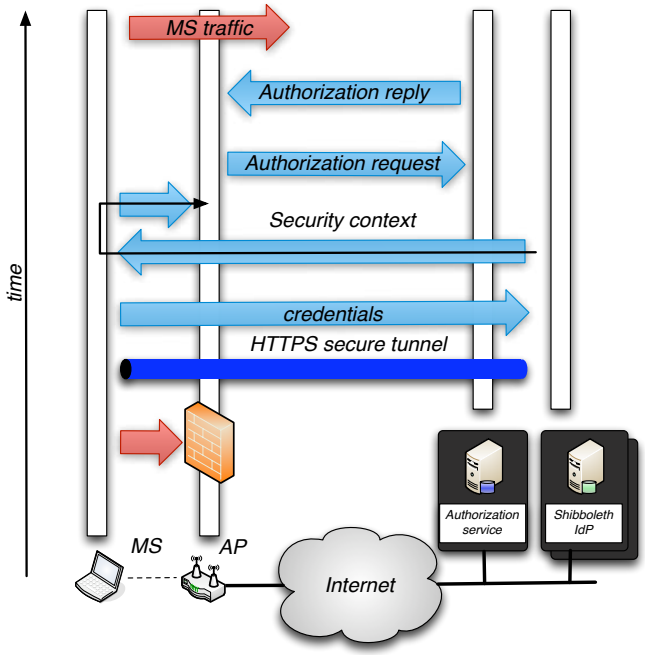

Figure 6. SWITCHaai protected Captive Portal

We now present the current architecture of the SWITCHaai protected Captive Portal (cf., Figure 6). The difference between the SWITCHaai architecture and the NAS AAA architecture is that the Shibboleth IdP server returns a security context to the AP, being a service provider in this scenario. Once, the AP possesses the information about authenticated user, the AP asks the Authorization service for permission to open the Internet connection for the MS. If the authorization service positively replies, the AP reconfigures its firewall, and thus the MS obtains full access to the Internet. As in the NAS model, the MS has a network address from the beginning and the credentials are sent over a secure channel, so the architecture is eavesdropping protected. The MS only presents credentials at home organization.

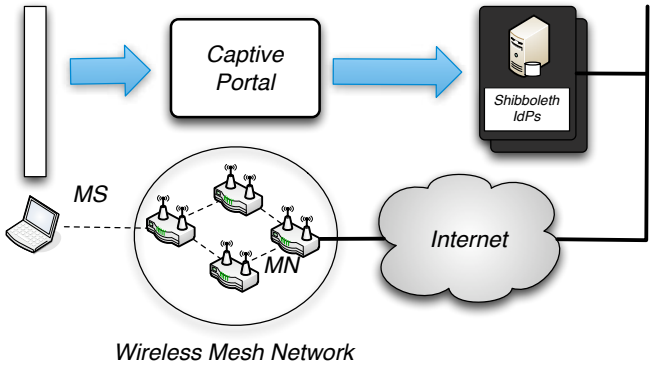

Figure 7. SWITCHaai protected Captive Portal by using WMNs

Because the wired infrastructure is expensive and limits the operational range, we propose to use WMNs as a complement or extension to wired networks. In this situation, a node delivering a signal to end users does not need to be directly connected to the wired infrastructure. In order to protect the wireless network, we design AAAA mechanisms compatible with WMNs. We present a Captive Portal solution being simple and compatible with the software installed on the majority of client machines (cf., Figure 7).

II. Wireless Mesh Network Architecture

For the proposed A^4 Mesh architecture, we distinguish different building elements: Authorization service, IdPs, Gateways (GWs), Master server, MNs and MSs (cf., Figure 8). MNs and MSs only use wireless communication, but GWs have both wired and wireless interfaces to provide the Internet connection to all-wireless stations. GWs and MNs form a wireless backhaul delivering a signal to MSs being end users or clients of our network. Each MS has a single owner, a human being running the device. The MS' owner is recognized by its digital identity. A MS is a client willing to use network resources, having a compatible hardware interface. MSs get connectivity to the Internet by associating themselves with MNs running access point like services. If the digital identity is recognized, it gives rights to use network resources. By analogy to MSs, each MN and GW has its own digital identity. MNs and GWs are responsible for building the network infrastructure, providing resources and extending network coverage. The architecture provides a single, easily expandable WMN, in which GWs, MNs, and MSs belong to one or many organizations (the Shibboleth federation). A single Master server is responsible for granting access to the network based on assertions from IdPs and the Authorization service. Our network is built upon the Internet Protocol (IP). At the beginning of operation, each node (GW, MN, MS) obtains a network local unique IP address (i.e., within the WMN) from the Master server. The WMN runs a routing protocol like: AODV, OLSR, 802.11s, etc. so that every packet

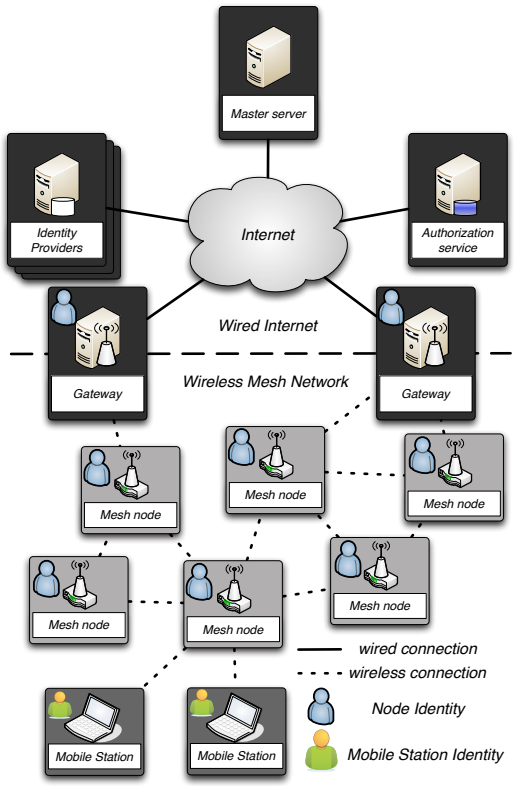

Figure 8. A^4 Mesh Architecture

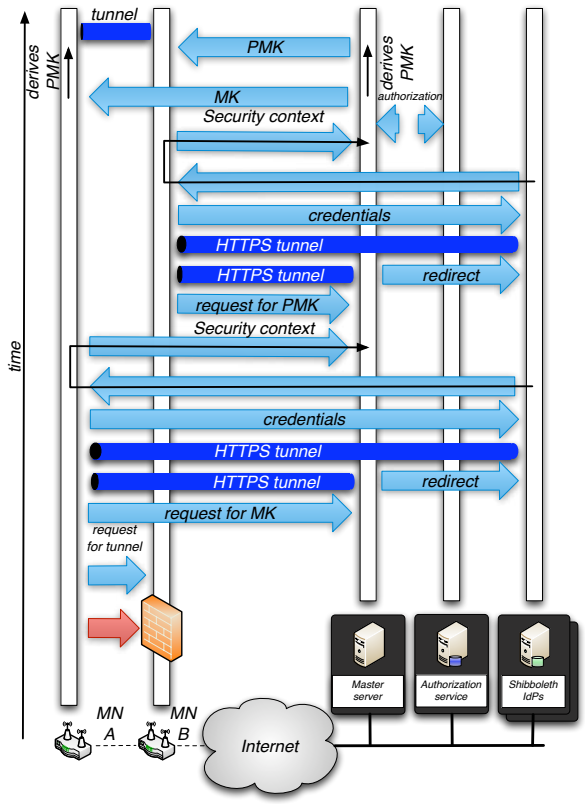

Figure 9. MN to MN operation

originated at the GW, MN or MS can reach the destination if the path exists. Only GWs and MNs are responsible for packet forwarding, MSs are end points of information flows.

A. Mesh Node to Mesh Node function

In the following, we describe an example of the operation between two MNs being immediate neighbors (cf., Figure 9). When two MNs sense each other, they can exchange messages by using their wireless interfaces. Imagine that MN A sends a data packet to MN B. At the beginning B only accepts signaling, routing protocol packets, or requests originated at or destined to the Master server or Shibboleth IdPs. Other traffic is dropped by the firewall at MN B. Note that the routing protocol is working in the network, because its traffic is accepted and exchanged between communicating MNs. We allow full communication between a pair of intermediate neighbors only if a secure tunnel is established. To establish a secure tunnel, one of the MNs (MN A) sends a "request for tunnel" signaling packet to its neighbor and visits the Master server (key server) to obtain a MK for communication between MN A and MN B. The master server redirects request to the IdP at which the MN authenticates itself sending credentials. The second MN (MN B) obtains the request for tunnel. It is obliged to ask the Master server for the PMK suitable for MN A-MN B communication. Requesting at the Master server, it is also redirected to the IdPs to authenticate itself. Once the authentication process is finished, the Master server possesses a security context based on the authentication of MN A and MN B. Based on the security context, the Master server asks the Authorization service for permission to establish a secure tunnel, between MN A and MN B. If the permission is granted, the Master server issues the MK and derives the PMK. MN A obtains the MK and MN B gets the PMK. MN A derives the PMK, so starting from this moment MN A and MN B both have the PMK being a symmetric key and they establish a secure tunnel. In a normal network operation, each MN establishes secure tunnels with every neighboring MN so that every packet originated at a MN can reach its destination in the WMN or Internet. Not authorized MNs cannot exchange traffic with neighboring nodes and thus they cannot inject traffic into the wireless backhaul.

In terms of a performance, we can distinguish several costs of this configuration, i.e., packet forwarding, routing overhead and key management. The cost of packet forwarding is high, because each consecutive node along the way towards the destination encrypts and decrypts the forwarded packet, however, the usage of symmetric cryptography is not so computationally exhausting. We do not introduce the routing overhead, because MNs can communicate along the shortest or most efficient paths. The key management is also at a reasonable level, because each node maintains $O(d)$ different keys, where d is the number of the node's immediate neighbors. Our organization of the wireless backhaul is obviously very flexible and we just

presented a single specification out of many other possibilities. We can use different methods. One possible replacement is that each MN gets the same key after successful authentication and authorization. In this case the backhaul would be protected by a single key and consecutive encryptions and decryptions at each hop are not necessary. In a different example, each node only maintains a secure tunnel with the Master server, so it increases the forwarding efficiency, however, reduces the routing performance, because the Master server has to forward traffic between MNs exchanging data packets. In another solution, we can exchange keys between any pair of communicating MNs, however, this increases the cost of key management, because each node maintains $O(N)$ keys, where N is the number of MNs in the network. We are going to implement several methods to protect the wireless backhaul against unlegitimate users and a more detailed performance analysis will be available in the future work.

B. Mesh Node to Mobile Node function

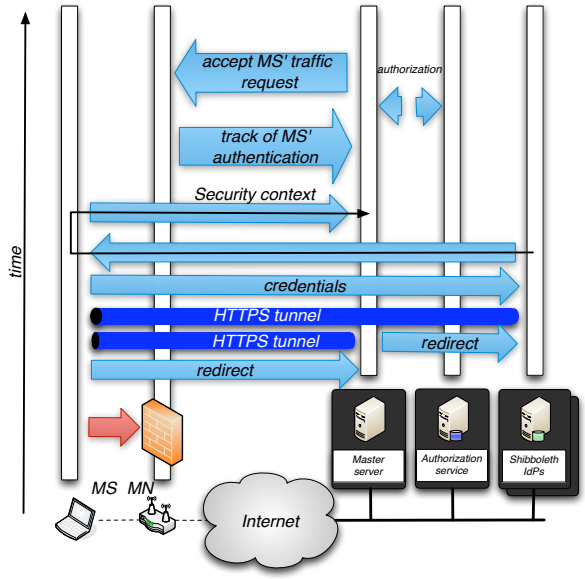

Figure 10. MS to MN operation

The Captive Portal functionality is illustrated in Figure 10. When a MS associates with a MN its traffic is blocked by a firewall running at the MN. In the initial phase, when the MS is using a web browser, all HTTP requests are redirected to the Master server to establish a HTTPS connection. Note that firewalls at every consecutive MN accept traffic going to the Master server and IdPs. The Master server redirects the request to the IdP to perform the user authentication. The MN sends credentials to the IdP so that the IdP creates a security context at the Master server. The MN bordering with the MS keeps track of the MS' authentication messages, e.g., by computing hashes of the IP packets and sending them to the Master server. By comparing the received hashes with its own track, the Master server exactly knows which of MNs provides a signal to the successfully authenticated MS. The Master server asks the Authorization service for permission to grant the MS full access to the Internet. When the Authorization service confirms that the MS can use the connection, the Master server requests the MN to reconfigure the firewall to accept the MS' traffic and updates its internal relation between the MS' IP address and the client identity running the MS (at every moment, the Master server exactly knows who is occupying a given IP address). To conclude, a firewall at the MN is a key point for the overall network security. Once, a MN accepts a packet coming from a MS and forwards it further over the secure channel to the intermediate MNs, the forwarding nodes do not make any other security checks related to the packet origin.

III. Accounting System

Accounting is a very important part of the A^4 Mesh architecture. From the general perspective its objective is to bookkeep resources consumed by MSs. Notice, that a single packet originated at a MS can be forwarded in a multi-hop way consuming resources at several MNs. The task relies now in tracking this consumption. In the current state, the SWITCHaai/Shibboleth architecture does not natively support accounting, however, in the future it will deliver a method of transporting the accounting information between two communicating entities: the Master server and an accounting server in the Internet performing the long term data storage. Each MN is responsible for accounting at short term with a high granularity and sending the accounting information to the Master server.

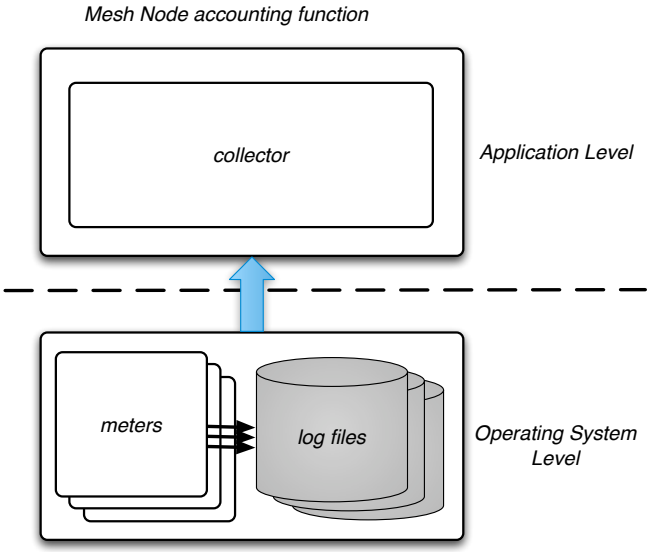

Figure 11. Mesh Node accounting architecture

Based on [12], we define the MN accounting function including metering, collecting and sending information to the Master server (cf., Figure 11). A MN runs a meter, a program that gathers and puts statistics to a local log-file. A MN's collector is a process taking the data from the

log-file and sending it to the Master server by using the accounting protocol. When the Master server gets records stored by MNs, they only contain the information on the forwarded flows identified by the IP addresses within the WMN. The Master server derives an identity responsible for the particular consumption of the network resources by virtue of the IP address-Identity relation. Starting from this moment, the Master server is able to issue accounting messages to the Accounting server containing resources consumed by a particular user.

IV. WMN Network Monitoring and Management

Our AAAA capable WMN is built out of MNs extending an Intranet (e.g., a University network) to distant areas in which the access to the network is mandatory, but ordinary wired networks are not available. Furthermore, it shall be possible to include MN nodes placed in remote areas (e.g., in mountain regions) where they are instrumental, e.g., for environmental measurements [2]. Because in such a case some of the MNs are not easily accessible, the network should be reliable and have a good network management and monitoring system. We now give a brief technical description of our network.

A. Mobile Stations and Mesh Nodes

There are no special requirements for MSs. They only require a standard Institute of Electrical and Electronics Engineers (IEEE) 802.11 adapter to join the network. Some of the MNs can be solar-powered, so energy efficient operation is required. To guarantee a continuous operation, a solar panel must be able to recharge a battery during its daily operation to compensate the 24 h energy consumption. MNs are usually built upon embedded hardware platforms. In our scenario, we use ALIX boards from PCEngines. The boards contain a single 500 MHz, i586 compatible CPU, 256 MB RAM, two wireless IEEE 802.11n interfaces Wistron DNMA-92, an Ethernet controller and a CompactFlash (CF) card. The platform has several important advantages: it is small, cheap, energy efficient, it does not contain moving mechanical elements like coolers or disks affected by failures. It can operate with a DC power source delivering 7V - 20V. To prevent from CF card failures, we want to limit writing cycles on the CF card as much as possible, as the heavy and long term operation on the memory card may quickly destroy it. In case of a failure, an on-board watchdog device can reboot the system. We use a very lightweight, tailored version of the Linux operating system. The ADAM Linux distribution [14] contains only relevant programs and it can be easily extended with a new software. Contrary to mesh nodes, gateways and other parts of our system located in the Internet are built out of high performance desktop systems. A gateway possesses wired and wireless interfaces in order to connect the WMN to the wired Internet.

[2]The installation of a WMN equipped with various sensors for capturing hydrogeological data in a remote mountain region [13] serves as test environment for the A^4 Mesh architecture.

B. Network Monitoring and Management

The monitoring operation enables detecting different reasons of failures. Imagine a situation in which a solar panel is broken and it does not charge a battery. To prevent from a node failure, the monitoring system generates alarms to warn a network administrator about a dangerous situation. Even if the administrator does not have enough time to react and the node dies as soon as its battery is empty, the administrator has a good knowledge about broken components and is able to quickly repair the system (fault management). From the more general perspective, system oriented statistics allow us to compute an average system accessibility and compare it with parameters of wired network devices. Link oriented statistics reflect the performance of the network.

In order to deal with all accounting objectives from Section III, we use a system collecting and sending accounting information to the Master server. We can reuse this system for network monitoring purposes in which each MN is responsible for gathering specific data classes:

- system oriented monitoring
- link level oriented monitoring

The first class contains system oriented parameters like the remaining battery time, power consumption, solar panel power, CPU and memory usage, number of processes, uptime, watchdog resets etc.

The second class is link oriented. MNs communicate by using the IEEE 802.11n cards. In order to measure the link performance, we use different techniques (e.g., active, passive, hybrid) [15]. We accumulate different statistics about the wireless medium and use this information in the future to optimize a routing decision, channel allocation or to alarm, e.g., that a link is broken. Many studies on Wireless Mesh Networks proved that it is difficult to operate a high performance WMN using simple hop count or latency metrics in the routing decisions [16]. The wireless medium is too complex for that [17] (cf., Section I). We gather the following information: a list of immediate neighbors, received signal strength, different link quality metrics like: ETX–average number of packet retransmissions [18], ETT–average time spend on packet transmission, i.e., a wireless medium active usage [19], air-time metric [20], etc., β–metric–link burstiness [21]. These metrics approximate the wireless link quality. We also try to distinguish the reasons of packet losses among: collisions, hidden nodes problems and noise errors [22].

In our scenario, we have the long range operating links, however a long distance has a degrading influence on the link performance, because the MAC medium sharing mechanism does not satisfactorily work under this condition. IEEE 802.11 CSMA/CA introduces specific time scales like DIFS, SIFS, Timeslots limiting the operational range to a few kilometers [23].

V. Related work

Much work concerns AAAA related issues in WMNs. Cheikhrouhou *et al.* [24] adapted IETF Protocol for carrying Authentication for Network Access (PANA) designed to

transmit EAP messages over the IP for WMNs. When a MS is authorized, it establishes an Internet Protocol Security (IPSec) tunnel with an enforcement point to get access to the Internet. Khan *et al.* [25] designed a MS-MN authentication function based on PANA and EAP-TTLS. After successful authorization a MS establishes a secure tunnel with a MN based on symmetric-key cryptography. Martignon *et al.* [26] proposed a two step associating function. In the first step a MS/MN associates itself with a network by using a classical IEEE 802.11i EAP-TLS mechanism. When a MN successfully passes the first step, it can upgrade its role in the network by accessing the key protected wireless backhaul. The MN needs to authenticate itself against a Key Server. After successful authentication, the MN gets the key and joins the backhaul. From the other perspective, fair and distributed accounting architectures like [27], [28] allow us to measure sent and forwarded traffic per MN. However, the architectures are distributed, the MNs cannot lie about their network activity because of a sophisticated protocol interacting between MNs and a trusted server.

VI. Conclusion

In this paper, we have described a simple AAAA oriented WMN architecture. The main contributions include an easily expandable wireless mesh network running the Captive Portal, which grants access to the Internet. We designed a protected network of MNs forwarding user traffic in a secure manner. A user authenticates itself against his home organization IdP, so the credentials are not exposed to third parties. Once a user is successfully authenticated, the bordering MN allows MS traffic to enter the wireless backhaul. Finally, the accounting system counts all resources consumed by the user network activity enabling further auditing and billing. Our architecture fits well IP based networks, because entire communication uses HTTP protocol, unlike EAP-RADIUS, which requires PANA to handle authentication messages.

Acknowledgments

The A4-Mesh project is carried out as a part of the program "AAA/SWITCH - e-Infrastructure for e-Science" lead by SWITCH, the Swiss National Research and Education Network, and is supported by funds from the Swiss State Secretariat for Education and Research. We thank Torsten Braun and his team for the most valuable collaboration in this work.

References

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47, no. 4, pp. 445–487, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/B6VRG-4F53V5H-2/2/9fa1587e47665f1fb3f7fb461461dd6b

[2] J. Bicket, D. Aguayo, S. Biswas, and R. Morris, "Architecture and evaluation of an unplanned 802.11b mesh network," in *MobiCom '05: Proceedings of the 11th annual international conference on Mobile computing and networking*, New York, NY, USA, 2005, pp. 31–42.

[3] IEEE, *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements*. Institute of Electrical and Electronics Engineers, July 2004.

[4] D. Mitton and M. Beadles, "Network access server requirements next generation (nasreqng) nas model," Internet Engineering Task Force, RFC 2881, July 2000. [Online]. Available: http://tools.ietf.org/rfc/rfc2881.txt

[5] D. Mitton, "Network access servers requirements: Extended radius practices," Internet Engineering Task Force, RFC 2882, July 2000. [Online]. Available: http://tools.ietf.org/rfc/rfc2882.txt

[6] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible authentication protocol (eap)," Internet Engineering Task Force, RFC 3748, June 2004. [Online]. Available: http://tools.ietf.org/rfc/rfc3748.txt

[7] D. Simon, B. Aboba, and R. Hurst, "The eap-tls authentication protocol," Internet Engineering Task Force, RFC 5216, March 2008. [Online]. Available: http://tools.ietf.org/rfc/rfc5216.txt

[8] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote authentication dial in user service (radius)," Internet Engineering Task Force, RFC 2865, June 2000. [Online]. Available: http://tools.ietf.org/rfc/rfc2865.txt

[9] C. Rigney, "Radius accounting," Internet Engineering Task Force, RFC 2866, June 2000. [Online]. Available: http://tools.ietf.org/rfc/rfc2866.txt

[10] C. Graf, U. Kienholz, T. Lenggenhager, M.-A. Steinemann, A. Redard, and D. Isch, "Aai - authentication and authorization infrastructure system and interface specification," SWITCH, System Specs, January 2004. [Online]. Available: http://www.switch.ch/aai/docs/AAI_System_Specs.pdf

[11] S. Carmody, M. Erdos, K. Hazelton, W. Hoehn, R. L. Morgan, T. Scavo, and D. Wasley, "Shibboleth architecture - protocols and profiles," Internet2, Architecture Specs, September 2005. [Online]. Available: http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-arch-protocols-latest.pdf

[12] C. Mills, D. Hirsh, and G. Ruth, "Internet accounting: Background," Internet Engineering Task Force, RFC 1272, November 1991. [Online]. Available: http://tools.ietf.org/rfc/rfc1272.txt

[13] R. Weingartner, "Montanaqua: Approaching water stress in the alps, water management options in the crans-montana-sierre region (valais, switzerland)," 2010. [Online]. Available: http://www.montanaqua.ch

[14] T. Staub, S. Morgenthaler, D. Balsiger, P. K. Goode, and T. Braun, "Adam: Administration and deployment of adhoc mesh networks," in *3rd IEEE Workshop on Hot Topics in Mesh Networking (IEEE HotMESH 2011), Lucca, Italy*, June 2011.

[15] K.-H. Kim and K. G. Shin, "On accurate measurement of link quality in multi-hop wireless mesh networks," in *MobiCom '06: Proceedings of the 12th annual international conference on Mobile computing and networking*, New York, NY, USA, 2006.

[16] D. S. J. De, C. Daniel, A. Benjamin, A. Chambers, and R. Morris, "Performance of multihop wireless networks: shortest path is not enough," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 1, January 2003.

[17] T. Liu, A. Kamthe, L. Jiang, and A. Cerpa, "Performance evaluation of link quality estimation metrics for static multihop wireless sensor networks," in *SECON '09: Proceedings of the 6th annual international conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2009, pp. 1–9.

[18] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of the 9th annual international conference on Mobile computing and networking*, New York, NY, USA, 2003, pp. 134–146.

[19] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," in *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*, New York, NY, USA, 2004, pp. 114–128.

[20] IEEE, *Draft STANDARD for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 1: Mesh Networking*. Institute of Electrical and Electronics Engineers, December 2010.

[21] K. Srinivasan, M. A. Kaz, S. Agarwal, and P. Levis, "The β-factor: Measuring wireless link burstiness," in *SenSys '08 Proceedings of the*

6th ACM conference on Embedded network sensor systems, New York, NY, USA, 2008, pp. 29–42.

[22] D. J. Leith and D. Malone, "Field measurements of 802.11 collision, noise and hidden-node loss rates," in *WiOpt '10 Proceedings of the 8th Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, 2010.

[23] R. Patra, S. Nedevschi, S. Surana, A. Sheth, L. Subramanian, and E. Brewer, "Wildnet: Design and implementation of high performance wifi based long distance networks," in *NSDI'07: Proceedings 4th USENIX Symposium on Networked Systems Design & Implementation*, April 2007, pp. 87–100.

[24] O. Cheikhrouhou, M. Laurent-Maknavicius, and H. Chaouchi, "Security architecture in a multi-hop mesh network," in *SAR'06: Proceedings of the 5th Conference on Security and Network Architectures*, June 2006.

[25] K. Khan and M. Akbar, "Authentication in multi-hop wireless mesh networks," in *16th Intl. Conference on Computer Science and Engineering (CISE 2006)*, 2006.

[26] F. Martignon, S. Paris, and A. Capone, "Mobisec: a novel security architecture for wireless mesh networks," in *Q2SWinet '08: Proceedings of the 4th ACM symposium on QoS and security for wireless and mobile networks*, October 2008.

[27] E. R. Cruz, D. Camara, and H. C. Guardia, "Providing billing support in wimax mesh networks," in *WIMOB '09: Proceedings of the 2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, October 2009.

[28] N. B. Salem, L. Buttyán, J.-P. Hubaux, and M. Jakobsson, "A charging and rewarding scheme for packet forwarding in multi-hop cellular networks," in *MobiHoc '03 Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, June 2003.